IN THE SPECIFICATION

Please replace the paragraph beginning at page 3, line 8 with:

In accordance with a first aspect of the invention, a given user device has associated therewith key pairs ~~(s, p) and~~ (s', p') and (s, p) corresponding to respective first and second digital signature protocols. The first digital signature protocol is preferably suitable for "fast" signature generation and has a computational efficiency compatible with the resources of a lightweight user device. The second digital signature protocol may be an arbitrary protocol, and may have a computational efficiency substantially lower than that of the first digital signature protocol. As part of a setup process, an agreement relating to the public keys p and p' is signed by both the user device and the intermediary device, and the resulting twice-signed agreement is stored by both the user device and the intermediary device. A first digital signature $s1$ is generated on a message m or a hash $h(m)$ thereof in the user device using the secret key s' and is sent to the verifier. The verifier in turn sends $s1$ to the intermediary, and the intermediary checks that $s1$ is a valid digital signature for the user device. If $s1$ is valid, the intermediary device generates a second digital signature $s2$ on m or $h(m)$ using the secret key s, and $s2$ is then returned to the verifier as a signature generated by the user device.